UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/844,448	04/27/2001	Gregory Neil Houston	05456.105005	9082

7590 10/21/2004

W. Scott Petty, Esq.
KING & SPALDING
45th Floor
191 Peachtree Street, N.E.
Atlanta, GA 30303

EXAMINER	
SON, LINH L D	

ART UNIT	PAPER NUMBER
2135	

DATE MAILED: 10/21/2004

Please find below and/or attached an Office communication concerning this application or proceeding.

Office Action Summary	Application No.	Applicant(s)	
	09/844,448	HOUSTON ET AL.	
	Examiner	Art Unit	
	Linh Son	2135	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If the period for reply specified above is less than thirty (30) days, a reply within the statutory minimum of thirty (30) days will be considered timely.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *27 April 2001*.

2a)☐ This action is **FINAL**. 2b)☒ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-59* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-59* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☐ The drawing(s) filed on _____ is/are: a)☐ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☒ Information Disclosure Statement(s) (PTO-1449 or PTO/SB/08) Paper No(s)/Mail Date *See Detail action*.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____ .
5) ☐ Notice of Informal Patent Application (PTO-152)
6) ☐ Other: _____.

DETAILED ACTION

1. This is a response to the Preliminary Amendment received on 07/27/2001.

2. Examiner accepts the IDS filed on the following dates: 05/14/2004, 04/28/2003, 01/22/2003, and 04/12/2002.

Claim Rejections - 35 USC § 103

3. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

4. Claims 1-59 are rejected under 35 U.S.C. 103(a) as being unpatentable over Trcka et al, US Patent No. 6453345B2, hereinafter "Trcka".

5. As per claims 1, 16, 25, 34, and 35, Trcka discloses a method for managing security event data collected from a security devices in a distributed computing environment (Col 5 lines 25-37) comprising the steps of: creating scope criteria for filtering security event data (Col 13 lines 1-15); generating security event data from a security devices located at a first location (Col 9 lines 5-45); collecting security event data at a second location (Col 5 lines 30-35, and Col 9 lines 48-59); and applying the scope criteria to the security event data at a third location to produce a result (Col 13

lines 1-31), the result accessible by a clients coupled to a server (Col 5 lines 35-37, Col 7 lines 50-67, and Col 11 lines 7-17). However, Trcka does not teach the implementation of more than one of the security devices collecting the data event in the network, and a plurality of clients coupled to a server to accessing the analyzed result. Nevertheless, It would have been obvious at the time of the invention for one having ordinary skill in the art to realize that having a plurality of security devices to collect event data in the network is profitable in term of processing power and detail collection of data packet. It would also have been obvious at the time of the invention for one having ordinary skill in the art to realize that a plurality of clients can access the server database to analyze the data since the http protocol is implemented (Col 7 lines 50-67).

6. As per claims 2 and 21, Trcka discloses the method of claims 1 and 16, further comprising storing one or more of the scope criteria and the result data (Col 23 lines 22-30).

7. As per claims 3 and 18, Trcka discloses the method of claims 1 and 16, wherein the first location is a distributed computing environment (Col 9 lines 5-45) and the second location is a database server (Col 5 lines 30-35, and Col 9 lines 48-59).

8. As per claims 4, 19, and 53, Trcka discloses the method of claims 1, 16, and 49, wherein collecting the security event data comprises generating security event data from a sensor (Col 10 line 60 to Col 11 line 4 and Col 12 line 65 to Col 13 line15);

sending the security event data from the sensor to a collector (Col 11 lines 27-47); and converting the event data to a common format (Col 12 lines 29-40).

9. As per claim 5, 20 and 30, Trcka discloses the method of claims 1 and 16. However, Trcka does not teach the analyzing is performed at an application server at the third location to which the plurality of clients are coupled. Nevertheless, It would have been obvious for one having ordinary skill in the art to realize that the analyzing software can be on a separate server. Having the analysis tool on a separate server will free the needed processing power for other software components (Col 10 lines 59-67) and also allow analyzing the captured event data for the clients more freely.

10. As per claims 6 and 39, Trcka discloses the method of claims 1 and 35, further comprising searching the stored security event data for additional information identifying a security event (Col 20 lines 1-17 and Col 18 lines 30-52).

11. As per claims 7 and 40, Trcka discloses the method of claims 1 and 35, further comprising: polling a database server for current stored security event data; analyzing the current stored security event data to produce current result data; and rendering the current result data (Col 20 lines 1-17 and Col 18 lines 30-52).

12. As per claims 8 and 41, Trcka discloses the method of claims 1 and 34, further comprising polling for messages containing information about scope criteria, security event data, or result data (Col 20 lines 1-17 and Col 18 lines 30-52).

13. As per claims 9 and 42, Trcka discloses the method of claims 1 and 34, further comprising pushing messages to a client wherein the messages contain information about scope criteria, security event data, or result data (Col 20 lines 1-17 and Col 18 lines 30-52).

14. As per claims 10, 17, and 43, Trcka discloses the method of claims 1 and 16, wherein the step of rendering result data comprises presenting the result data in a chart format (Col 20 lines 1-17 and Col 18 lines 30-52).

15. As per claims 11, 22, 44, and 55, Trcka discloses the method of claims 1, 16, and 34, wherein in response to analyzing the collected security event data, an action is executed (Col 20 lines 1-17 and Col 18 lines 30-52).

16. As per claims 12, 23, 45, and 56, Trcka discloses the method of claims 11, 22, and 44. However, Trcka does not mention the action is clearing security event data from storage. Nevertheless, it would have been obvious at the time of the invention for one having ordinary skill in the art to realize that the cabability of clearing out the data must

be exist in the invention of Trcka, since it is inevitable to contain unlimited data in any storage devices.

17. As per claims 13, 24, and 46, Trcka discloses the method of claims 11, 22, and 44, wherein the action is creating an incident from result data for preparing a response (Col 21 lines 3-55).

18. As per claims 14, 38, and 47, Trcka discloses the method of claims 1, 16, and 34, wherein the step of collecting security event data further comprises converting the data to a uniform format (Col 12 lines 29-40).

19. As per claims 15, 26-27, 48, and 59, Claim 16 rejection is incorporated. Further Trcka discloses an event manager coupled to the security devices (Col 10 line 59 to Col 11 line15), the event manager operable for collecting security event data from the security devices and analyzing the security event data (Col 11 lines 1-15); and a client coupled to the event manager, operable to perform an action in response to receiving analyzed security event data from the event manager (Col 12 line 65 to Col 13 line 15).

20. As per claim 28, Trcka discloses the system of claim 27, wherein the event manager comprises a database server operable for storing the collected security event data and the analyzed security event data (Fig 2 and 3, and Col 13 lines 1-15).

21. As per claim 29, Trcka discloses the system of claim 27, wherein the event manager comprises an application server operable for creating an incident from the security event data for preparing a response (Col 13 lines 1-15).

22. As per claim 31, Trcka discloses the system of Claim 27, wherein multiple clients operable for receiving analyzed security data are coupled to the event manager (Col 13 lines 1-15).

23. As per claim 32, Trcka discloses the method of Claim 27, wherein the action performed by the client is rendering a chart containing analyzed security event data (Col 13 lines 1-15).

24. As per claim 33, Trcka discloses the method of Claim 1, further comprising the step of rendering the result data in a manageable format for the plurality of clients (Col 13 lines 1-15).

25. As per claim 36, Claim 5 rejection is incorporated. Trcka discloses the method of Claim 34, wherein the first location is a distributed computing environment (Col 9 lines 5-45), and the second location is a database server (Col 5 lines 30-35, and Col 9 lines 48-59).

26. As per claim 37, Trcka discloses the method of Claim 34, further comprising editing the scope criteria (Col 13 lines 55-65).

27. As per claim 49, Claim 16 rejection is incorporated. Further, Trcka discloses responsive to the plurality of security devices, generating security event data (Col 13 lines 1-15); transferring the security event data from the security devices for storage in a database (Col 17 lines 9-23); and applying a scope criteria to the security event data to produce a result by filtering the security event data, the result accessible by a plurality of clients coupled to an application server (Col 17 lines 24-55 and Col 18 lines 30-52).

28. As per claim 50, Trcka discloses the method of Claim 49, further comprising rendering the result in a rendering for output to the clients (Col 20 lines 1-17 and Col 18 lines 30-52).

29. As per claim 51-52, Trcka discloses the method of Claim 49, further comprising the step of creating and editing the scope criteria for filtering the security event data (Col 13 lines 50-65).

30. As per claims 54, Trcka discloses the method of Claim 49, further comprising storing one or more of the scope criteria (Col 13 lines 50-65), the security event data (Col 13 lines 1-15), and the result in a database (Col 12 lines 9-10, and Fig 3, 90).

Conclusion

31. Any inquiry concerning this communication from the examiner should be directed to Linh Son whose telephone number is (703)-305-8914.

32. If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor Kim Y. Vu can be reached at (703)-305-4393. The fax numbers for this group are (703)-872-9306 (official fax). Any inquiry of general nature or relating to the status of this application or proceeding should be directed to the group receptionist whose telephone number is (703)-305-9600.

33. Please notice. Due to the Office moving, the telephone numbers above will only be valid until October 15th of 2004. After that, the follow list of numbers will be valid:

Examiner: (571) 272-3856.

Kim Y. Vu: (571) 272-3859

Receptionist : (571) 272-2100

34. Information regarding the status of an application may be obtained from the Patent Application Information Retrieval IPAIR.I system. Status information for published applications may be obtained from either Private PMR or Public PMR. Status information for unpublished applications is available through Private PMR only. For more information about the PAIR system, see http://pzr-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).

AU 2135

Linh LD Son

Patent Examiner